PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04Q 7/38 — A1

(11) Internationale Veröffentlichungsnummer: **WO 99/08466**

(43) Internationales Veröffentlichungsdatum: 18. Februar 1999 (18.02.99)

(21) Internationales Aktenzeichen: PCT/DE98/01943

(22) Internationales Anmeldedatum: 13. Juli 1998 (13.07.98)

(30) Prioritätsdaten:
197 33 662.0 4. August 1997 (04.08.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DE-TEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]; Landgrabenweg 151, D–53227 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: DUPRE, Michael [DE/DE]; Zedernweg 175, D–53757 Sankt Augustin (DE).

(74) Anwalt: RIEBLING, Peter; Postfach 31 60, D–88113 Lindau (DE).

(81) Bestimmungsstaaten: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CZ, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD AND DEVICE FOR CUSTOMER PERSONALIZATION OF GSM CHIPS

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR KUNDENSEITIGEN PERSONALISIERUNG VON GSM–CHIPS

(57) Abstract

The invention relates to a method for personalization of GSM chips. At least one subscriber identification character(IMSI) and a card number (ICCID) are stored in the memory area of said chips in addition to a secret key (Ki) and other optional data for personalization purposes. The invention aims to eliminate an unnecessarily high degree of complexity linked to management of all card data in an authentication centre (AC) and to preserve secret chip data in a more secure manner. According to the invention, final data is only written on the chip when the subscriber logs into a subscriber network. One advantage is that only initial data is written into the card enabling the customer to contact the computer centre of the information provider. During first contact the final data is traded between the card and the computer centre and written into the card. The computer centre is simply required to manage cards which have really been issued to customers.

(57) Zusammenfassung

Es wird ein Verfahren zur Personalisierung von GSM–Chips beschrieben, in deren Speicherbereich mindestens eine Teilnehmer–Kennung IMSI und eine Kartennummer ICCID eingespeichert ist, und wobei zwecks Personalisierung dem Chip noch ein geheimer Schlüssel Ki und ggf. weitere Daten eingespeichert sind. Es soll ein unnötig großer Verwaltungsaufwand zur Verwaltung aller Kartendaten im Authentifikationszentrum AC entfallen und die Aufbewahrung der geheimen Daten des Chips soll sicherer ausgebildet werden. Die Erfindung sieht vor, daß der Chip die endgültigen Daten erst dann eingeschrieben erhält, wenn der Teilnehmer sich in das Teilnehmernetz einbucht. Damit besteht der Vorteil, daß in die Karte lediglich anfängliche Daten eingeschrieben werden, mit denen der Kunde lediglich in der Lage ist, erstmalig mit dem Rechenzentrum des Netzbetreibers Kontakt aufzunehmen. Bei diesem erstmaligen Kontakt werden dann die endgültigen Daten zwischen der Karte und dem Rechenzentrum ausgehandelt und in die Karte eingeschrieben. Das Rechenzentrum braucht deshalb nur die Karten zu verwalten, die auch tatsächlich an Kunden vergeben wurden.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren und Vorrichtung zur kundenseitigen Personalisierung von GSM-Chips.

Beschreibung

Vorgeschlagen wird ein Verfahren zur kundenseitigen Personalisierung von GSM-Chips, bei dem davon ausgegangen wird, daß sich der Chip zum Zeitpunkt der Personalisierung im Endgerät des Kunden befindet.
Nach dem Stand der Technik ist der GSM-Chip bei den Netzbetreibern zur Zeit in einer GSM-Karte implementiert, die in das Endgerät eingesteckt wird. Dieser Chip könnte genausogut fest in das Endgerät integriert sein., z. B. auf einer Einschubkarte eines Computers. Bei dem vorliegenden Verfahren spielt es also keine Rolle, ob eine GSM-Karte oder ein Endgerät mit integriertem Chip verwendet wird. Unter dem Begriff "Chip" wird im weitesten Sinne ein EPROM, ein EEPROM oder auch ein "intelligenter" Mikroprozessor verstanden.

Ohne Beschränkung auf eine bestimmte Ausführungsform ist im folgenden von einem "Chip" und dem "Chiphersteller" die Rede.

Bei der bisherigen, zentralen Personalisierung erhält der Chip neben anderen Daten eine Kartennummer (ICCID), eine Teilnehmerkennung (IMSI) und mehrere Geheimzahlen eingeschrieben. Während der Chiphersteller ohne weiteres die Daten ICCID und IMSI in den Chip einbringen könnte, möchte der Netzbetreiber gerne selbst die Kontrolle über die Geheimzahlen, insbesondere über den Schlüssel Ki, der nur der Karte und dem Netz bekannt sein soll, behalten.

Bei der gegenwärtigen, zentralen Personalisierung bekommt der Netzbetreiber Rohkarten vom Kartenhersteller und schreibt dann den endgültigen, geheimen Schlüssel hinein. Dieser

Schlüssel ist dann nur zwei Stellen bekannt, nämlich dem Chip selbst und dem Netzbetreiber.
Nachteilig hierbei ist, daß im Rechenzentrum des Netzbetreibers eine außerordentlich hohe statische Last erzeugt wird. Mit einem Generator werden eine Vielzahl von Schlüsseln erzeugt, die dann in die jeweiligen Karten eingebracht werden. Man schickt dann gleichzeitig den jeweils pro Karte erzeugten Schlüssel zum Rechenzentrum (Authentifikationszentrum AC), und danach wird den Karte an die Verkaufsorganisationen herausgegeben. Das AC hat also im Moment der Herausgabe der jeweiligen Karte bereits alle Teilnehmerkennungen IMSI und die dazugehörenden geheimen Schlüssel Ki gespeichert und muß diese verwalten, obwohl die jeweilige Karte noch irgendwo beim Händler liegt und noch gar nicht verkauft worden ist. Bei einer größeren Anzahl von Verkaufsstellen liegen also Karten, die noch nicht verkauft wurden und deren Daten aber trotzdem vom AC verwaltet werden müssen.

Außerdem besteht prinzipiell die Gefahr, daß wenn ein Hersteller oder irgendein anderes Mitglied der Verkaufsorganisation die Karten personalisieren soll, es sein könnte, daß dieser Schlüssel kompromittiert ist. Die anfängliche Personalisierung des Chip ist also unsicher und mit der Gefahr des Mißbrauchs behaftet.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren, eine Vorrichtung und einen Chip der eingangs genannten Art so weiterzubilden, daß ein unnötig großer Verwaltungsaufwand im AC entfallen kann und daß die Aufbewahrung der geheimen Daten des Chip sicherer ausgebildet ist.

Zur Lösung der gestellten Aufgabe ist die Erfindung durch die technische Lehre des Anspruchs 1 gekennzeichnet. Ein Chip nach der Erfindung ist durch die technische Lehre der Ansprüche 6 bis 10 gekennzeichnet. Im übrigen wird die

Vorrichtung zur kundenseitigen Personalisierung des GSM-Chips in den Ansprüchen 11 bis 13 beschrieben.

Mit der erfindungsgemäßen technischen Lehre werden insbesondere folgende Vorteile erreicht :

- Vermeidung einer zentralen Personalisierung beim Netzbetreiber
- Ausgabe von sehr vielen GSM-Chips ohne Erzeugung einer statischen Last beim Netzbetreiber
- Wiederverwendung von "gebrauchten" GSM-Chips
- Regelmäßiger Wechsel des secret Key Ki während der Nutzungsdauer durch den Kunden.

Mit dem hier vorgestellten Verfahren bringt der Gerätehersteller/Chiphersteller initiale kartenbezogene Daten in den Chip ein, sozusagen eine Vorpersonalisierung. Die eigentliche Personalisierung nimmt der Netzbetreiber selbst zu einem späteren Zeitpunkt vor, und auch nur bei den Kunden, die ein Vertragsverhältnis mit dem Netzbetreiber eingehen.

Die Vorpersonalisierung erzeugt bei dem Netzbetreiber noch keine statische Last. Das Verfahren bietet somit die Voraussetzung, um "Millionen" von GSM-Chips zu verteilen, z. B. in jedes Auto, in jeden Laptop oder in jede Alarmanlage, und später nur die Chips der Kunden zu "aktivieren", die ein Vertragsverhältnisse eingehen.

Des weiteren ist es möglich, Karten wiederzuverwenden, falls ein Kunde sein Vertragsverhältnis kündigt (z. B. bei Verkauf seines Autos).

Speziell beim Netzbetreiber D1 könnte der Händler zurückgegebene Karten erneut für einen anderen Kunden freischalten. Der Netzbetreiber spart somit die Personalisierung von Karten für das Austauschgeschäft ein.

Zur Verwirklichung der technischen Lehre wird es bevorzugt, wenn der GSM-Chip Toolkit fähig ist. Insbesondere sollte das Endgerät Short Messages zum Netzbetreiber schicken können. Außerdem sollte der Chip eine Funktion anbieten, den Chip wieder initial zu machen (s. u.)
Im übrigen kann auch das Endgerät oder ein anderes Gerät diese Funktion des Chip nutzen
Die Kartennummer und die Versionsnummer (s. u.) sollten durch das Endgerät auslesbar sein (oder auf der GSM-Karte sichtbar sein).

Der Chiphersteller ist für die Vorpersonalisierungzuständig. ICCID und IMSI werden einem Nummernpool entnommen, der Chip selbst leitet sich aus einem Schlüssel K1, den der Chiphersteller kennt, einen initialen Ki_1 ab. PIN und PUK werden auf einen Defaultwert gesetzt.
- Im AC erfolgt kein Eintrag
- Wird ein Kunde gewonnen, erfolgt ein Eintrag im AC. Dieses leitet sich ebenfalls den initialen Key Ki_1 ab.
- Im HLR wird das Hotlining Flag gesetzt
- Der erste Call wird zu einem Security Center geroutet
- Dieses handelt mit dem Verfahren nach Diffie-Hellman einen neuen Ki_2 sowie einen PUK aus.
- Gebrauchte Chips, die wiederverwendet werden sollen, werden mit einer internen Funktion zurückgesetzt.

Die Vorpersonalisierung beim Chiphersteller erfolgt dergestalt, daß jeder Chiphersteller einen Bereich von Kartennummern und Teilnehmerkennungen zugeteilt bekommt. Die Nummernbereiche für ICCID und IMSI sind so groß, daß dies möglich ist.
Weiterhin erhält der Chiphersteller folgende Daten vom Netzbetreiber: a, p, VER, K1

Der Chiphersteller bringt dann folgende Daten in jeden Chip ein:

- ICCID Kartennummer
- IMSI Teilnehmerkennung (ist an ICCID gebunden, z. B. gleiche Position innerhalb der beiden Nummernbereiche für ICCID und IMSI)
- a hinreichend große Zahl, Basis für Diffie Hellman.
- p hinreichend große Zahl, Primzahl für Diffie Hellman
- VER Versionsnummer, z. B. 8 Byte, eindeutig je Chiphersteller (kann öfters gewechselt werden)
- K1 8 Byte DES-Schlüssel, eindeutig an VER gebunden

Bemerkung: Der Netzbetreiber könnte sich mit einem Masterkey den Schlüssel K1 aus der Versionsnummer VER ableiten (z. B. mit DES-Verfahren). Dies ist aber nicht notwendig.

Der Chip generiert sich dann folgende Geheimzahlen:

- Ki_1 Ki_1 ist ein initialer Ki, den der Chip mit dem DES-Schlüssel K1 aus der IMSI ableitet.
- PIN Die PIN wird fest auf 0000 gesetzt
- PUK Der PUK wird fest auf 00000000 gesetzt
- ggf. weitere Geheimzahlen

Der Chip muß K1 und die generierten Geheimzahlen in einem sicheren Bereich halten und vor Auslesen schützen.

Die Vorgänge im Authentifikationszentrum AC:

- Das AC kennt von jeder Versionsnummer VER den Schlüssel K1 (kann K1 mit einem Masterkey aus VER abgeleitet werden, brauchen die an die Chipherstellern ausgegebenen K1 nicht gespeichert zu werden)
- Die von den Chips generierten initialen Ki_1 werden nicht in das AC eingetragen

Das AC kennt auch die IMSIs noch nicht, somit ist keine statische Last vorhanden

Kundengewinnung und Freischaltung durch den Netzbetreiber

Möchte ein Kunde sein Gerät (seine Karte, seinen Chip) nutzen, geht er mit dem Netzbetreiber einen Vertrag ein. Die Kartennummer (ICCID) identifiziert den Chip.

Der Netzbetreiber veranlaßt folgende Aktionen:

- Auslesen oder Ablesen von Kartennummer und Versionsnummer (ICCID, VER)
- Der ICCID ist die IMSI fest zugeordnet
- im AC werden IMSI und VER eingetragen (jetzt erst wird das Teilnehmerverhältnis im AC bekannt gemacht)
- Das AC kennt den Schlüssel K1, der fest an VER gebunden ist und generiert sich aus K1 den initialen Schlüssel Ki_1 nach dem gleichen Verfahren, das im Chip verwendet wurde, aus der IMSI
- Das HLR setzt das "Hotlining Flag" zu dieser IMSI. Der erste Call geht dann zu einem SC (Security Center) (das SC könnte auch das HLR/AC selbst sein)

Der erste Call: Endpersonalisierung des Chip

- Da der Chip und das AC jetzt den gleichen secret Key Ki_1 kennen, bucht der Chip im Netz ein (Die PIN ist 0000 und dem Kunden bekannt)
- Der erste Call wird wegen Hotlining automatisch zum SC geroutet. Je nach Software im toolkit-fähigen Endgerät könnte der erste call bereits eine Short Message sein
- *Das SC nutzt die Toolkitfähigkeit des Chip aus und handelt mit dem Chip einen neuen secret key Ki_2 aus.*

Hierbei wird das Verfahren nach Diffie Hellmann verwendet, das folgende Vorteile bietet:

* beliebig lange Keys sind aushandelbar
* Abhören auf der Luftschnittstelle reicht nicht aus, den generierten Schlüssel auszuspähen

Der Chip speichert den neuen Key Ki_2 ab (dieser wird im folgenden zur Authentikation verwendet).

- Der neue Key kann sofort verifiziert werden (z. B. challenge respone wie bei GSM üblich)
- Das SC überträgt den neuen Ki_2 an das AC
- Ebenfalls per Diffie Hellman handelt das SC auch einen PUK (oder weitere Geheimzahlen) mit dem Chip aus. (Der Netzbetreiber kann dem Kunden die Geheimzahlen anschließend mitteilen oder auch für Service-Zwecke selbst behalten)
- Im HLR wird das Hotlining Flag entfernt. Damit sind jetzt reguläre Calls möglich, wobei ab diesem Zeitpunkt der neue secret Key Ki_2 verwendet wird
- Das toolkitfähige Endgerät informiert den Kunden über Erfolg oder Mißerfolg
- Das toolkitfähige Endgerät könnte dem Kunden anbieten, die PIN neu zu setzen

<u>Wiederverwendung gebrauchter Chips / Karten</u>

Sei das Teilnehmerverhältnis im HLR und AC ausgetragen, weil der Kunde gekündigt hat. Bei Vertragsabschluß mit dem neuen Kunden und dem gebrauchten Chip muß folgendes geschehen:

Zuerst wird die Funktion des Endgeräts zum Initialisieren des Chips genutzt. Daraufhin wird im Chip:

- Ki_2 wird gelöscht
- Ki_1 wird wieder aktiviert
- die PIN wird auf 0000 gesetzt
- der PUK wird auf 00000000 gesetzt (analog mit weiteren Geheimzahlen PUK2)

Diese Funktion könnte innerhalb des D1-Netzes beispielsweise der *X13 aktivieren*, der bei vielen Händlern steht. Damit hat der Händler wieder eine initiale Karte zum Vergeben.

Weiter geht es wie bei Kundengewinnung und Freischaltung durch den Netzbetreiber (s. o.)

Wechsel des secret key während der Nutzungsdauer des Chip

Der Netzbetreiber hat die Möglichkeit, in regelmäßigen Abständen einen Wechsel des Ki zu erzwingen. Dazu reicht es aus, im HLR das Hotlining-Flag zu setzen, den Call zum SC zu routen und wie oben beschrieben einen neuen Ki auszuhandeln. Der PUK sollte diesmal jedoch nicht neu ausgehandelt werden.

Mögliche Mißbrauchsszenarien (hier für D1 dargestellt)

1. Der Schlüssel K1 eines Chipherstellers ist kompromittiert und eine Karte wird nachgemacht

1.1 Die IMSI ist im AC noch nicht bekannt
Die Karte bucht nicht ein

1.2 Die IMSI der echten Karte ist bereits im AC und wurde bereits endpersonalisiert
Die falsche Karte bucht nicht ein, da Ki_1 ungleich Ki_2 ist (Authentikation gescheitert)

1.3 Die echte IMSI ist bereits im AC, wurde aber noch nicht endpersonalisiert

Dies ist der kurze Zeitraum zwischen Vertragsabschluß und erstem Einschalten des Geräts. In dieser Zeit könnte sich eine Kartenfälschung "dazwischenschieben". Die echte Karte würde danach nicht einbuchen können, da sie nicht den Ki_2 der Fälschung besitzt. Dieses Szenario könnte organisatorisch vermieden werden, z.B. indem bei der Subscription eine Geheimzahl auf das Auftragsformular

geschrieben wird, die der Kunde nach dem Schlüssel-Aushändigen eingeben muß, die zum SC geschickt wird und dort geprüft wird.

2. Der Kunde macht seine eigene Karte initial (z. B. mit X13) Die Karte hat danach den Ki_1 und bucht nicht mehr ein.

Die Erfindung wird nun anhand eines Ausführungsbeispiels anhand der Zeichnungen näher beschrieben. Hierbei gehen aus den Zeichnungen und ihrer Beschreibung weitere Merkmale und Vorteile hervor.

Es zeigen:

Figur 1: Schematisiert die Vorpersonalisierung der Karten beim Kartenhersteller;

Figur 2: Schematisiert die Vorgänge beim Freischalten durch den Netzbetreiber (Endpersonalisierung);

Figur 3: Schematisiert die Vorgänge beim Löschen des Chips und bei der Wiederverwendung.

In Figur 1 ist zeichnerisch dargestellt, was bereits schon auf Seite 4 der Beschreibung angegeben ist, daß nämlich die Kartennummer ICCID in einem Bereich von einer Zahl X bis zu einer Zahl Y vorliegt.

Gleiches gilt für die Teilnehmerkennung IMSI, die ebenfalls in einem Zahlenbereich von A-B vorliegt.

Innerhalb der beiden Nummernbereiche für die ICCID und für die IMSI wird ferner eine Zahl a als Basis für die Diffie Hellman gewählt und ebenso eine Zahl p, die als Primzahl für die Diffie Hellman-Verschlüsselung dient.

Es wird ferner eine VER definiert, die als Funktionsnummer 8 Byte lang sein kann und ferner wird der Schlüssel K1 als DES-Schlüssel errechnet, der an VER gebunden ist.

Die genannten Daten werden in die Karte eingeschrieben und hierbei generiert (errechnet) der Chip dann die Geheimzahl Ki_1, welche in der Karte gespeichert wird. Die Karte wird in dieser Form (Vorpersonalisierung) an die VO (Verkaufsorganisation) ausgeliefert.

In Figur 2 sind die einzelnen Vorgänge beschrieben, die ab Seite 5 der Beschreibung dargestellt sind.

Die VO geht in einem ersten Verfahrensschritt mit dem Kunden einen Vertrag ein. Im gleichen Verfahrensschritt wird die Kartennummer ICCID und die Versionsnummer in einer Auftragsbestätigung zusammen mit dem Vertrag eingetragen und diese Auftragsbestätigung wird in einem zweiten Verfahrensschritt zusammen mit der Teilnehmerkennung und der Versionsnummer VER an das AC mitgeteilt.

Gleichzeitig wird durch Mitteilung der Teilnehmerkennung IMSI an das HLR dafür gesorgt, daß das HLR die Kartendaten zur Kenntnis erhält und das sogenannte Hotlining Flag einrichtet.

Der Kunde erhält nun seine vorpersonalisierte Karte und nimmt mit dem ersten Anruf - der im Sinne der vorliegenden Erfindung zwangsläufig auf das SC geschaltet ist - Kontakt mit dem SC auf, wobei bei diesem ersten Anruf die Ki_2 ausgehandelt wird, ebenso wie die PUK und gleichzeitig wird auch die PIN neu gesetzt. Das SC andererseits verifiziert die geheime Schlüsselzahl Ki_2 gegenüber der Karte.

In einem vierten Verfahrensschritt nimmt SC Kontakt mit dem HLR auf und entfernt das Hotlining Flag, was dem Kunden nun die Möglichkeit gibt, beliebige Calls abzusetzen.

Das SC teilt im vierten Verfahrensschritt gleichzeitig die geheime Schlüsselzahl Ki_2 dem AC mit.

Damit ist die Karte freigeschaltet und endpersonalisiert.

Die Wiederverwendung gebrauchter Karten ist auf Seite der Beschreibung näher dargestellt. Hierbei ist in Figur 3 erkennbar, daß der Kunde mit seiner Karte sich an die VO wendet, welche durch Eintragung der Kartennummer ICCID in die Auftragsbestätigung dafür sorgt, daß im AC die IMSI gelöscht wird und gleichzeitig auch im HLR.

Damit wird auch die Ki_2 gelöscht und die Ki_1 wird wieder aktiviert und in die Karte eingespeichert. Ebenso wird die PIN auf den Wert OOOO gesetzt und ebenfalls die PUK.

Die so wieder vorpersonalisierte Karte kann denn in einen Kartenpool eingestellt werden und für neue Kunden vergeben werden.

Die Endpersonalisierung wurde also wieder rückgängig gemacht und des liegt wieder der Zustand der Karte vor, wie er zum Zeitpunkt der Vorpersonalisierung bestand.

Es sei noch angemerkt, daß die Stelle des Netzbetreibers, bei welcher die Auftragsbestätigung abgewickelt wird, als Auftragsannahmestelle bezeichnet wird und diese Auftragsannahmestelle kennt die Zuordnungen von ICCID zu IMSI wegen der 1:1-Zuordnung innerhalb des vergebenen Nummernbereiches.

Patentansprüche

1. Verfahren zur Personalisierung von GSM-Chips, in deren Speicherbereich mindestens eine Teilnehmer-Kennung IMSI und eine Kartennummer ICCID eingespeichert ist, und wobei zwecks Personalisierung dem Chip noch ein geheimer Schlüssel Ki und gegebenenfalls weitere Daten eingespeichert sind, **dadurch gekennzeichnet, daß** die Personalisierung des Chips dann erfolgt, wenn der Teilnehmer sich in das Teilnehmernetz einbucht.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, daß** die Personalisierung des Chips dann erfolgt, wenn der Teilnehmer sich erstmals in das Teilnehmernetz einbucht.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, daß** zur Vorpersonalisierung des Chips beim Hersteller zunächst initiale, kartenbezogene Daten, nämlich ein erster, geheimer Schlüssel Ki_1 und gegebenenfalls weitere Daten, wie PIN und PUK eingespeichert werden.

4. Verfahren nach einem der Ansprüche 1-3, **gekennzeichnet durch** folgende Verfahrensschritte :

in einem ersten Verfahrensschritt entnimmt der Chiphersteller die ICCID und IMSI einem Nummernpool, der Chip selbst leitet sich aus einem Schlüssel K1, den der Chiphersteller kennt und in den Chip einbringt, einen initialen Ki_1 ab, PIN und PUK werden auf einen Defaultwert gesetzt,

in einem zweiten Verfahrensschritt erfolgt ein Eintrag im AC und HLR, sobald ein Teilnehmer einen Vertrag mit dem Netzbetreiber geschlossen hat,

in einem dritten Verfahrensschritt leitet sich das AC ebenfalls den initialen, ersten Schlüssel Ki_1 ab

in einem vierten Verfahrensschritt setzt das Netz die Bedingungen, damit beim Einbuchen ins Netz eine Verbindung vom Chip zur Komponente SC (Security Center des Netzbetreibers) entsteht,

in einem fünften Verfahrensschritt wird beim ersten Einbuchen die Verbindung vom Chip zum SC geschaltet

in einem sechsten Verfahrensschritt wird im SC ein neuer, zweiter, geheimer Schlüssel Ki_2, sowie gegebenenfalls ein PUK mit dem Chip ausgehandelt (z.B. mit dem Verfahren nach Diffie-Hellman) oder im SC erzeugt und zum Chip übertragen

in einem siebten Verfahrensschritt werden die Bedingungen aus Verfahrensschritt 4 wieder ausgeschaltet.

5. Verfahren nach einem der Ansprüche 1-4, **dadurch gekennzeichnet, daß** der erstmalig in den Chip eingespeicherte, initiale, geheime Schlüssel Ki_1 vor Vertragsabschluß nicht in das AC übertragen und dort gespeichert wird.

6. Chip zur Ausübung des Verfahrens nach einem der Ansprüche 1-5, **dadurch gekennzeichnet, daß** der Chip im Endgerät toolkitfähig ist , und mit dem SC kommunizieren kann und einen Schlüssel aushandeln kann.

7. Chip nach Anspruch 6, **dadurch gekennzeichnet, daß** der Chip Daten aus dem SC empfangen kann und diese in seinen Speicher einschreibt und gegebenenfalls aus dem Speicher ausliest, verändert und/oder an das Rechenzentrum (SC) überträgt.

8. Chip nach einem der Ansprüche 6 oder 7, **dadurch gekennzeichnet, daß** sein Mikroprozessor einen geheimen Schlüssel mit dem SC aushandelt.

9. Chip nach Anspruch 8, **dadurch gekennzeichnet, daß** zum

Aushandeln des Schlüssels des Verfahrens das Verfahren nach Diffie-Hellman ist.

10. Chip nach einem der Ansprüche 6-9, **dadurch gekennzeichnet, daß** der Chip eine vom Hersteller fest programmierte Rufnummer enthält (fixed dialing).

11. Rechenzentrum zur Ausübung des Verfahrens nach einem der Ansprüche 1-5, **dadurch gekennzeichnet, daß** das HLR geeignet ist, einen Umleitungsbefehl (Hotlining-Flag) zu setzen und zu löschen.

12. Rechenzentrum zur Ausübung des Verfahrens nach einem der Ansprüche 1-5, unter Verwendung eines Chips nach einem der Ansprüche 6-10, **dadurch gekennzeichnet, daß** das Netz die Bedingungen setzt, damit beim Einbuchen ins Netz eine Verbindung vom Chip zur Komponente SC entsteht.

13. Rechenzentrum zur Ausübung des Verfahrens nach einem der Ansprüche 1-5, unter Verwendung eines Chips nach einem der Ansprüche 6-10, **dadurch gekennzeichnet, daß** mit der erstmaligen Eintragung des initialen Schlüssel Ki_1 in das AC auch das Hotlining flag im HLR gesetzt wird.

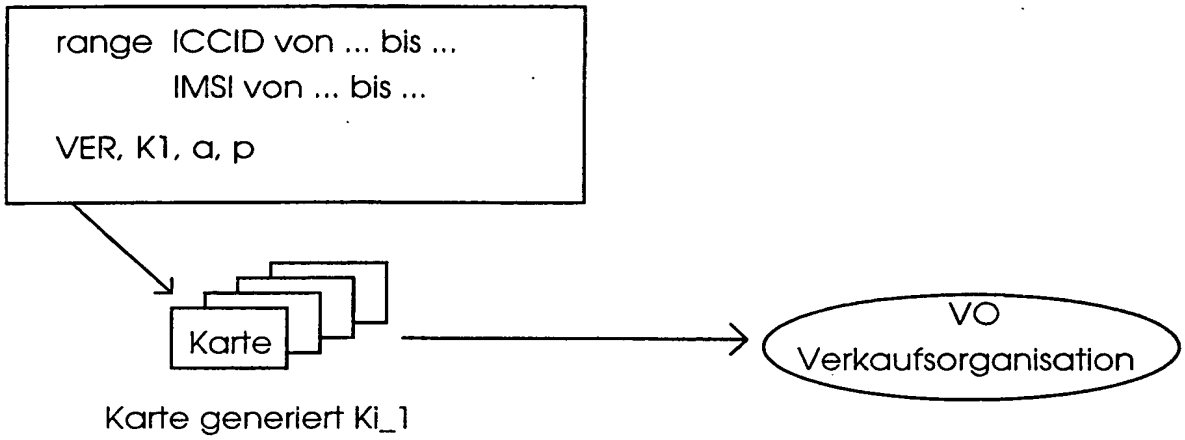
range ICCID von ... bis ...
IMSI von ... bis ...
VER, K1, a, p
Karte
VO
Verkaufsorganisation
Karte generiert Ki_1

Fig. 1

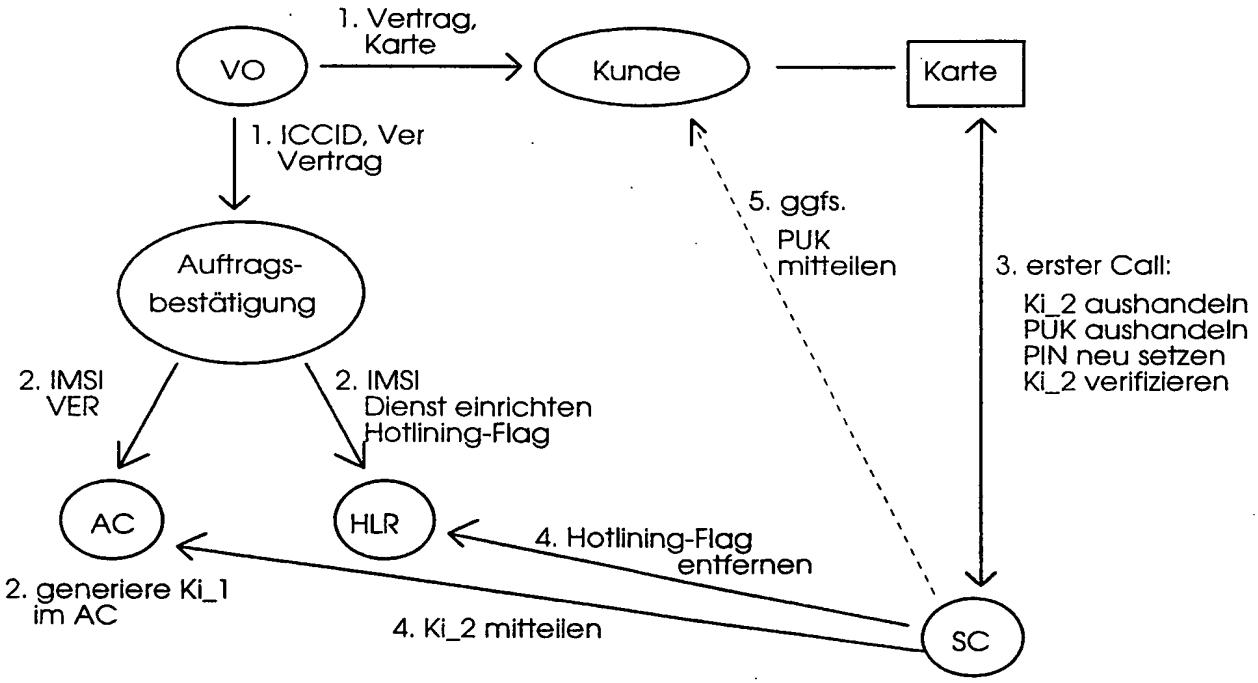
VO
1. Vertrag, Karte
Kunde
Karte
1. ICCID, Ver Vertrag
Auftrags-bestätigung
5. ggfs. PUK mitteilen
3. erster Call:
Ki_2 aushandeln
PUK aushandeln
PIN neu setzen
Ki_2 verifizieren
2. IMSI VER
2. IMSI Dienst einrichten Hotlining-Flag
AC
HLR
4. Hotlining-Flag entfernen
2. generiere Ki_1 im AC
4. Ki_2 mitteilen
SC

Fig. 2

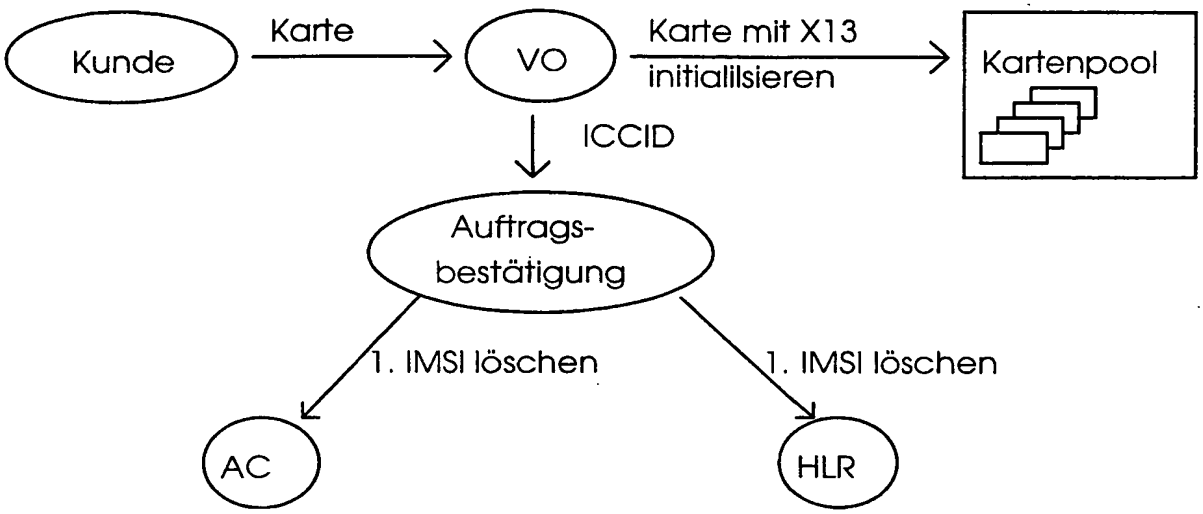
Kunde
Karte
VO
Karte mit X13
initialilsieren
Kartenpool
ICCID
Auftrags-
bestätigung
1. IMSI löschen
1. IMSI löschen
AC
HLR

Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/01943

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 93 07697 A (COMVIK GSM AB) 15 April 1993 see page 3, line 4 - page 7, line 11 ---	1-9,12
X	WO 97 14258 A (QUALCOMM INC) 17 April 1997 see page 10, line 15 - page 21, line 30 ---	1,2, 5-10,12
X	EP 0 481 714 A (VODAFONE LTD) 22 April 1992 see column 3, line 15 - column 6, line 9 ---	1-3, 11-13
X	EP 0 562 890 A (HUTCHISON MICROTEL LIMITED) 29 September 1993 see column 2, line 41 - column 6, line 57 ---	1
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 December 1998	14/12/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Roberti, V

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/01943

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	EP 0 820 206 A (AT & T WIRELESS SERVICES INC) 21 January 1998 see column 4, line 45 - column 13, line 42	1,2

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE 98/01943

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9307697	A	15-04-1993	SE	468068 B	26-10-1992
			AU	661048 B	13-07-1995
			AU	2699092 A	03-05-1993
			CA	2115435 A,C	15-04-1993
			DE	606408 T	16-03-1995
			EP	0606408 A	20-07-1994
			FI	940804 A	21-02-1994
			JP	6511125 T	08-12-1994
			NO	940473 A	16-02-1994
			NZ	244523 A	27-02-1996
			SE	9102835 A	26-10-1992
			SG	44338 A	19-12-1997
			US	5557679 A	17-09-1996
WO 9714258	A	17-04-1997	AU	7442696 A	30-04-1997
			CA	2234558 A	17-04-1997
			EP	0855125 A	29-07-1998
EP 0481714	A	22-04-1992	GB	2248999 A	22-04-1992
			AT	147223 T	15-01-1997
			DE	69123931 D	13-02-1997
			DE	69123931 T	30-04-1997
			DK	481714 T	16-06-1997
			ES	2096635 T	16-03-1997
			FI	914917 A	18-04-1992
			GR	3022655 T	31-05-1997
			IE	65966 B	29-11-1995
			NO	180811 B	24-03-1997
			PT	99263 A	31-01-1994
EP 0562890	A	29-09-1993	NONE		
EP 0820206	A	21-01-1998	BR	9703967 A	04-08-1998
			CA	2208601 A	15-01-1998
			JP	10117385 A	06-05-1998
			NO	973157 A	16-01-1998

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/01943

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04Q7/38

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 93 07697 A (COMVIK GSM AB) 15. April 1993 siehe Seite 3, Zeile 4 - Seite 7, Zeile 11 ---	1-9,12
X	WO 97 14258 A (QUALCOMM INC) 17. April 1997 siehe Seite 10, Zeile 15 - Seite 21, Zeile 30 ---	1,2, 5-10,12
X	EP 0 481 714 A (VODAFONE LTD) 22. April 1992 siehe Spalte 3, Zeile 15 - Spalte 6, Zeile 9 ---	1-3, 11-13
X	EP 0 562 890 A (HUTCHISON MICROTEL LIMITED) 29. September 1993 siehe Spalte 2, Zeile 41 - Spalte 6, Zeile 57 ---	1

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
8. Dezember 1998	14/12/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Roberti, V

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/01943

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	EP 0 820 206 A (AT & T WIRELESS SERVICES INC) 21. Januar 1998 siehe Spalte 4, Zeile 45 - Spalte 13, Zeile 42	1,2

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER [redacted]CHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Im [redacted]ionales Aktenzeichen
PCT/DE 98/01943

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9307697	A	15-04-1993	SE	468068 B	26-10-1992
			AU	661048 B	13-07-1995
			AU	2699092 A	03-05-1993
			CA	2115435 A,C	15-04-1993
			DE	606408 T	16-03-1995
			EP	0606408 A	20-07-1994
			FI	940804 A	21-02-1994
			JP	6511125 T	08-12-1994
			NO	940473 A	16-02-1994
			NZ	244523 A	27-02-1996
			SE	9102835 A	26-10-1992
			SG	44338 A	19-12-1997
			US	5557679 A	17-09-1996
WO 9714258	A	17-04-1997	AU	7442696 A	30-04-1997
			CA	2234558 A	17-04-1997
			EP	0855125 A	29-07-1998
EP 0481714	A	22-04-1992	GB	2248999 A	22-04-1992
			AT	147223 T	15-01-1997
			DE	69123931 D	13-02-1997
			DE	69123931 T	30-04-1997
			DK	481714 T	16-06-1997
			ES	2096635 T	16-03-1997
			FI	914917 A	18-04-1992
			GR	3022655 T	31-05-1997
			IE	65966 B	29-11-1995
			NO	180811 B	24-03-1997
			PT	99263 A	31-01-1994
EP 0562890	A	29-09-1993	KEINE		
EP 0820206	A	21-01-1998	BR	9703967 A	04-08-1998
			CA	2208601 A	15-01-1998
			JP	10117385 A	06-05-1998
			NO	973157 A	16-01-1998